An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606180236

NCSC Advisory

Critical Vulnerability in Cisco Catalyst SD-WAN Manager

CVE-2026-20127

18th, June 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-20127

Published: 2026-02-25

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Manager

CVSS Score[1]: 10

Products Affected

This vulnerability affects Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Manager, and Cisco Catalyst SD-WAN Validator, regardless of device configuration.

This vulnerability affects the following deployment types:

- On-Prem Deployment
- Cisco Hosted SD-WAN Cloud
- Cisco Hosted SD-WAN Cloud - Cisco Managed
- Cisco Hosted SD-WAN Cloud - FedRAMP Environment

As there is an extensive list of Software version affected, we ask that you please refer to the vendors own advisory to find out if your product is affected.

Impact

A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.

This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to an affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF,

[1] https://www.first.org/cvss/

which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.

Common Weakness Enumeration (CWE)[2]: CWE-287: Improper Authentication

Known Exploited Vulnerability (KEV) catalog[3]: Yes

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2026-20127
- https://www.cve.org/CVERecord?id=CVE-2026-20127
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-20127

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog